UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,719	09/08/2006	Agostinho De Arruda Villela	2171323-000002	9289

44777   7590   04/28/2009
W. EDWARD RAMAGE
COMMERCE CENTER SUITE 1000
211 COMMERCE ST
NASHVILLE, TN 37201

EXAMINER
WRIGHT, BRYAN F

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _14 January 2009_.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _17-35_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _17-35_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

FINAL ACTION

1.   This action in response to Amendment filed 1/14/2009. Claims 17, 31-35 are

amended. Claims (17-35) are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 17, 18, 22-27, 29, 30, 31 and 35 are rejected under 35 U.S.C. 103(a) as

being unpatentable over by Schwartz et al (US Patent Publication No. 20010044896

and Schwartz hereinafter) and Kato (US Patent Publication No. 2002/0184385) in view

of Bajkar (US Patent Publication No. 2005/0133582) and further in view of Matzuzeki

(WO 2004/023275 (cited from IDS)).

3.   As to claim 17, Schwartz teaches a method for identifying devices and controlling

access to a service, comprising the steps of:

        sending the digital signature of the device to the authentication server (e.g.,

external system) [col. 16, lines 5-20];

Schwartz does not expressly teach the claim limitation element of collecting data related

to software and hardware configurations from the device through a software agent;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Kato. Kato discloses

the claim limitation element of collecting data related to software and hardware

configurations from the device through a software agent (to provide device configuration

capturing capability [par. 158]:

Therefore, given the teachings of Kato, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

Schwartz by employing the well known feature of capturing device configuration data

disclosed above by Kato, for which digital signature generation will be enhanced [par.

158].

The combination of Schwartz and Kato does not expressly teach the claim limitation

element of generating a digital signature for the device by hashing the software and

hardware configuration data;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz and Kato as

introduced by Bajkar. Bajkar discloses the claim limitation element of generating a

digital signature for the device by hashing the software and hardware configuration data

(to provide digest value generating capability of hardware and software configuration

data [par. 55]).

Therefore, given the teachings of Bajkar, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

the combination of Schwartz and Kato by employing the well known feature of capturing

device configuration data disclosed above by Bajkar, for which digital signature

generation will be enhanced [par. 55].

The combination of Schwartz, Kato and Bajkar does not teach the claim limitation element of determining whether the device has been excluded from accessing or enrolling in the service.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schwartz, Kato and Bajkar as introduced by Matsuzaki. Matsuzaki teaches the claim limitation element of determining whether the device has been excluded from accessing or enrolling in the service (to provide determining means for determining legitimate devices for electronic transaction (e.g., accessing services) [fig. 9]).

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schwartz, Kato and Bajkar by employing the well known feature of access control based on the number of current enrollees disclosed above by Matsuzaki, for which access control will be enhanced [fig, 9].

4.   As to claim 18, Schwartz teaches a method where the digital signature sent to the authentication sewer is encrypted (i.e., … teaches encrypting the digital signature Schwartz provides the encryption capability [par. 109]).

5.   As to claim 22, Schwartz teaches a method where the authentication server

compares the digital signature sent with one or more previously-stored digital signatures

(i.e., … teaches the capability to compare digital signatures [par. 102]).

6.   As to claim 23, Schwartz teaches a method where the authentication server

determines whether the device has been excluded from accessing or enrolling in the

service by determining whether the device is on a list or in a group of devices not

allowed to access the service, or is included within a group of devices allowed to access

the service (i.e., … teaches to authenticate a device on the base of access criteria

stored in database [par. 88]).

7.   As to claims 24 and 25, the system disclosed by Schwartz shows substantial

features of the claimed invention (discussed in the paragraphs above), it fails to

disclose:

        A method where the authentication server allows a maximum number of

enrollments for a particular device (claim 24).

        A method where the maximum number of enrollments is zero (claim 25).

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Matsuzaki.

Matsuzaki discloses:

A method where the authentication server allows a maximum number of enrollments for a particular device (claim 24) (for purposes of allowing a maximum number of device enrolled device Matsuzaki provides the capability to limit the number of devices enrolled [abstract]).

A method where the maximum number of enrollments is zero (claim 25) for purposes of allowing a maximum number of device enrolled device Matsuzaki provides the capability to limit the number of devices enrolled [abstract]).

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of device registration disclosed above by Matsuzaki, for which controlling access to services will be enhanced [abstract].

8.   As to claim 26, Schwartz teaches a method where the authentication server allows minor modifications to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device (i.e., .. .teaches a control policy for which allows modification to configuration within authentication guidelines [par. 94]).

9.   As to claim 27, Schwartz teaches a method where the previously-stored digital

signature of the device is updated to reflect the modifications (i.e., ... teaches modifying

to invalidate previously stored signature and invalidate previously stored signature with

new signatures [par. 78].

10.   As to claims 29 and 30, the system disclosed by Schwartz shows substantial

features of the claimed invention (discussed in the paragraphs above), it fails to

disclose:

        A method where multiple devices can be registered for a single user with the

authentication server to create a registration hierarchy (claim 29).

        A method where a user can unregister a device only through the device itself, or

another device within the registration hierarchy registered earlier than the device to be

unregistered (claim 30).

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Matsuzaki.

Matsuzaki discloses:

        A method where multiple devices can be registered for a single user with the

authentication server to create a registration hierarchy (claim 29) (for purposes of a

registration hierarchy Matsuzaki provides registration hierarchy for registering devices

[fig. 16].

A method where a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered (claim 30) (for purpose of unregistering a device Matsuzaki provides decision capability to determine device status according to registration information [pg. 19, lines 10-25].

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of device registration disclosed above by Matsuzaki, for which controlling access to services will be enhanced [abstract].

11.   As to claim 31 , Schwartz teaches a method for identifying devices and controlling access to a service, comprising the steps of:

sending the digital signature of the device to the authentication server [par. 39];

verifying that the device is not on a list (e.g. control policy) or in a group of devices not allowed to access the service (i.e., .. teaches a control policy and device record for verification and determining access privileges [par. 90; par. 94]), or is not a device with a maximum number (e.g., critical threshold) of enrollments set to zero (i.e., ... teaches a critical threshold [par. 100]);

and registering the device as authorized to access the service [fig. 3; par. 86]

Schwartz does not expressly teach the claim limitation element of collecting data related

to software and hardware configurations from the device through a software agent;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Kato. Kato discloses

the claim limitation element of collecting data related to software and hardware

configurations from the device through a software agent (to provide device configuration

capturing capability [par. 158]:

Therefore, given the teachings of Kato, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

Schwartz by employing the well known feature of capturing device configuration data

disclosed above by Kato, for which access control will be enhanced [par. 158].

The combination of Schwartz and Kato does not expressly teach the claim limitation

element of generating a digital signature for the device by hashing the software and

hardware configuration data;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz and Kato as

introduced by Bajkar. Bajkar discloses the claim limitation element of generating a

digital signature for the device by hashing the software and hardware configuration data

(to provide digest value generating capability of hardware and software configuration

data [par. 55]).

Therefore, given the teachings of Bajkar, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

the combination of Schwartz and Kato by employing the well known feature of capturing

device configuration data disclosed above by Bajkar, for which access control will be

enhanced [par. 55].

The combination of Schwartz, Kato and Bajkar does not expressly teach the claim

limitation element of:

      verifying that the device is not on a list or in a group of devices not allowed to

access the service or is not a device with a maximum number of enrollments set to

zero;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz, Kato and Bajkar

as introduced by Matsuzaki. Matsuzaki discloses

      verifying that the device is not on a list or in a group of devices not allowed to

access the service or is not a device with a maximum number of enrollments set to

zero (to provide access control capability based on verifying number of enrollees [S56,

fig. 9];

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at

the time of the invention would have recognized the desirability and advantage of

modifying the combination of Schwartz, Kato and Bajkar by employing the well known

feature of access control based on the number of current enrollees disclosed above by

Matsuzaki, for which access control will be enhanced [par. 55].

12.   As to claim 35 , Schwartz teaches a method for identifying devices and

controlling access to a service, comprising the steps of:

        an authentication server that determines whether the device can access the

service based upon the digital signature of the device [par. 39];

        and registering the device as authorized to access the service [fig. 3; par. 86]

Schwartz does not expressly teach the claim limitation element of a software agent

installed on a device, adapted to collecting data related to software and hardware

configurations from the device through a software agent;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Kato. Kato discloses

the claim limitation element of a software agent installed on a device, adapted to

collecting data related to software and hardware configurations from the device through

a software agent (to provide device configuration capturing capability [par. 158]:

Therefore, given the teachings of Kato, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

Schwartz by employing the well known feature of capturing device configuration data

disclosed above by Kato, for which digital signature generation will be enhanced [par.

158].

The combination of Schwartz and Kato does not expressly teach the claim limitation

element of a digital signature for the device, generated by a software agent by hashing

the software and hardware configuration data;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz and Kato as

introduced by Bajkar. Bajkar discloses the claim limitation element of a digital signature

for the device, generated by a software agent by hashing the software and hardware

configuration data (to provide digest value generating capability of hardware and

software configuration data [par. 55]).

Therefore, given the teachings of Bajkar, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

the combination of Schwartz and Kato by employing the well known feature of capturing

device configuration data disclosed above by Bajkar, for which digital signature

generation will be enhanced [par. 55].

The combination of Schwartz, Kato and Bajkar does not expressly teach the claim

limitation element of:

  wherein the authentication server verifies that the device is not a list or in a group

of device not allowed to access the service, or is not a device with a maximum number

of enrollment set to zero,

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz, Kato and Bajkar

as introduced by Matsuzaki. Matsuzaki discloses

  wherein the authentication server verifies that the device is not a list or in a group

of device not allowed to access the service, or is not a device with a maximum number

of enrollment set to zero (to provide access control capability based on verifying number

of enrollees [S56, fig. 9];

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at

the time of the invention would have recognized the desirability and advantage of

modifying the combination of Schwartz, Kato and Bajkar by employing the well known

feature of access control based on the number of current enrollees disclosed above by

Matsuzaki, for which access control will be enhanced [par. 55].

13.   Claims 19-21 rejected under 35 U.S.C. 103(a) as being unpatentable over the

combination of Schwartz, Kato, Bajkar, and Matsuzaki, as applied to claim 17 above,

and further in view of Cui et al. (US Patent Publication No. 2005/0166053 and Cui

hereinafter).

14.   As to claims 19-21, although the combination of Schwartz, Kato, Bajkar, and

Matsuzaki illustrates substantial features of the claim invention, the combine teaching of

Schwartz, Kato, Bajkar, and Matsuzaki does not disclose:

        A method where the software agent is installed on the device as part of the

process of using the device to access a service (claim 19).

        A method where the hashes used to generate the digital signature are changed

with every attempt to access a service, and the hashes cannot be reversed (claim 20).

        A method where the digital signature is one of several stages of a framework of

authorization and authentication processes governing access to the service by the

device (claim 21).

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz, Kato, Bajkar and

Matsuzaki.as introduced by Cui. Cui discloses:

        A method where the software agent is installed on the device as part of the

process of using the device to access a service (claim 19) (to provide the user agent

(UA) executing on the mobile device [par. 53]).

A method where the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed (claim 20) (to provide one-way hash function capability such updating (rolling) the device signature(s) is based, in part, on a pre-determined period of time [par. 63; par. 70]).

A method where the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device (claim 21) (to provide access governing capability [fig. 3]).

Therefore, given the teachings of Cui, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schwartz, Kato, Bajkar and Matsuzaki by employing the well known feature of access control disclosed above by Cui, for which access control will be enhanced [fig, 5].

15.   Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Schwartz, Kato, Bajkar, and Matsuzaki, as applied to claim 17 above, and further in view of Wade et al. (US Patent No. 5,552,776 and Wade hereinafter).

16.   As to claim 28, the system disclosed by the combination of Schwartz, Kato, Bajkar, and Matsuzaki shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

A method where the authentication server logs all accesses or attempted accesses by a device to the service (claim 28)

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schwartz, Kato, Bajkar, and Matsuzaki as introduced by Wade. Wade discloses:

A method where the authentication server logs all accesses or attempted accesses by a device to the service (claim 28) (for purposes of logging access attempts Wade provides the capability login attempts [col. 9, lines 15-25]).

Therefore, given the teachings of Wades, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schwartz, Kato, Bajkar, and Matsuzaki by employing the well known features of limiting the number of enrolled devices disclosed above by Wades, for which controlling access to services will be enhanced [abstract].

17.   Claims 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Schwartz, Kato, Bajkar and Matsuzaki, as applied to claim 31 above, and further in view of Blumenau et al. (US Patent Publication No. 2002/0083339 and Blumenau hereinafter).

18.   As to claim 32, although the combined teaching of Schwartz, Kato, Bajkar and

Matsuzaki illustrates substantial features of the claim invention, the teachings of

Schwartz however does not disclose:

A method further comprising the step of verifying the identity of the device each

time it subsequently attempts to access the service.

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz, Kato, Bajkar and

Matsuzaki as introduced by Blumenau. Blumenau discloses:

A method further comprising the step of verifying the identity of the device each

time it subsequently attempts to access the service (to provide device identity for

subsequent access attempts [par. 7]).

Therefore, given the teachings of Blumenau, a person having ordinary skill in the art at

the time of the invention would have recognized the desirability and advantage of

modifying the combination of Schwartz, Kato, Bajkar and Matsuzaki by employing the

well known feature of verifying device identity for subsequent access attempts disclosed

above by Blumenau, for which digital signature generation will be enhanced [par. 55].

19.   As to claim 33, Schwartz teaches a method where the step of verifying the

identity of the device comprises the steps of:

and sending the digital signature of the device to an authentication server (i.e., ...

teaches send a device signature to a server for authentication [fig. 4]).

and comparing the digital signature sent with one or more previously- stored

digital signatures for the device [par. 78];

Schwartz does not expressly teach the claim limitation element of collecting data related

to software and hardware configurations from the device through a software agent;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Schwartz as introduced by Kato. Kato discloses

the claim limitation element of collecting data related to software and hardware

configurations from the device through a software agent (to provide device configuration

capturing capability [par. 158]:

Therefore, given the teachings of Kato, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

Schwartz by employing the well known feature of capturing device configuration data

disclosed above by Kato, for which access control will be enhanced [par. 158].

The combination of Schwartz and Kato does not expressly teach the claim limitation

element of generating a digital signature for the device by hashing the software and

hardware configuration data;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz and Kato as

introduced by Bajkar. Bajkar discloses the claim limitation element of generating a

digital signature for the device by hashing the software and hardware configuration data

(to provide digest value generating capability of hardware and software configuration

data [par. 55]).

Therefore, given the teachings of Bajkar, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

the combination of Schwartz and Kato by employing the well known feature of capturing

device configuration data disclosed above by Bajkar, for which access control will be

enhanced [par. 55].

20.   As to claim 34, Schwartz teaches a method where the step of verifying the

identity of the device comprises the steps of:

        and sending the digital signature of the device to an authentication server (for

purposes of signature authentication Schwartz provides the capability to send a device

signature to a server for authentication [fig. 4]).

Schwartz does not expressly teach the claim limitation element of collecting data related

to software and hardware configurations from the device through a software agent;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schwartz as introduced by Kato. Kato discloses the claim limitation element of collecting data related to software and hardware configurations from the device through a software agent (to provide device configuration capturing capability [par. 158]:

Therefore, given the teachings of Kato, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known feature of capturing device configuration data disclosed above by Kato, for which access control will be enhanced [par. 158].

The combination of Schwartz and Kato does not expressly teach the claim limitation element of generating a digital signature for the device by hashing the software and hardware configuration data;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schwartz and Kato as introduced by Bajkar. Bajkar discloses the claim limitation element of generating a digital signature for the device by hashing the software and hardware configuration data (to provide digest value generating capability of hardware and software configuration data [par. 55]).

Therefore, given the teachings of Bajkar, a person having ordinary skill in the art at the

time of the invention would have recognized the desirability and advantage of modifying

the combination of Schwartz and Kato by employing the well known feature of capturing

device configuration data disclosed above by Bajkar, for which access control will be

enhanced [par. 55].

The combination of Schwartz, Kato and Bajkar does not expressly teach the claim

limitation element of:

 verifying that the device is not on a list or in a group of devices not allowed to

access the service or is not a device with a maximum number of enrollments set to

zero;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by the combination of Schwartz, Kato and Bajkar

as introduced by Matsuzaki. Matsuzaki discloses

 verifying that the device is not on a list or in a group of devices not allowed to

access the service or is not a device with a maximum number of enrollments set to

zero (to provide access control capability based on verifying number of enrollees [S56,

fig. 9];

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schwartz, Kato and Bajkar by employing the well known feature of access control based on the number of current enrollees disclosed above by Matsuzaki, for which access control will be enhanced [par. 55].

Response to Arguments

Applicant's arguments with respect to claims 17-35 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-

3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431